REPORT TO THE BRITISH CHIEFS OF STAFF AND THE US CHIEFS OF STAFF OF THE UK/US COMMUNICATION SECURITY CONFERENCE ON THE REPLACEMENT OF THE CCM HELD AT WASHINGTON, D.C. COMMENCING 21 SEPTEMBER 1950

1. As agreed by the British and US Chiefs of Staff* a UK/US Conference to consider the replacement of the existing Combined Cypher Machine opened in Washington on the 21st September 1950, as a result of which the Senior British Representative recommends that the British Chiefs of Staff accept the offer by the U.S. Chiefs of Staff of the 7-rotor BCM principle as the long-term solution of the replacement for the present combined cypher machine (CCM).

2. Related cryptographic devices and features were demonstrated and discussed. Summaries of the proceedings at these meetings have been prepared and these are held both by the Director, Armed Forces Security Agency, Washington, and the Secretary, Cypher Policy Board, London. This Conference has been of unquestioned value in the field of Combined Communications Security.

3. It is recommended:

a. That immediately and on a continuing basis there be complete interchange of technical details of the devices discussed in this Conference. This should include technical visits.

* US Reference: JCS 2074/2 - 27 December 1949.
British Reference: COS(W)831 - 26 July 1950.

b. That there be annual conferences on this subject for the next four years, to be held alternately in London and in Washington, the first of these to take place in London in approximately nine months time. These conferences should be concurrent with conferences for the reciprocal exchange of cryptographic information.

c. That the subject of Combined requirements for general point-to-point on-line encryption be introduced at the next Conference.

4. The general recommendations in paragraph 3 above together with the detailed recommendations of the conference which are attached as Appendix A to this report are submitted for approval by the British and U.S. Chiefs of Staff.

[redacted]
Chairman, U.K. Delegation

EARL E. STONE
Rear Admiral, U.S. Navy
Chairman, U.S. Delegation

at Washington, D.C.
27 October 1950

APPENDIX A

DETAILED RECOMMENDATIONS

Replacement of the existing CCM

(a) That the cryptographic principles of the 7-rotor BCM (cryptosystem BRUTUS) be adopted as a replacement for the CCM in combined communications.

(b) That except by mutual agreement, disclosure of the BRUTUS principle be limited to the U.S. and to the nations of the British Commonwealth; and that the U.K. and the U.S. agree to notify each other when any issue of a combined BRUTUS system is made to another nation.

(c) That the target date for full implementation of BRUTUS be set as 1 January 1955, or sooner if circumstances permit, and that limited introduction, where a small number of machines would be involved, should be implemented at the earliest practicable date.

(d) That insofar as practicable rotors of U.S. and British versions of the BRUTUS cryptosystem ~~be~~ be physically and cryptographically interchangeable and that to this end the British should adopt one or more of the sizes to be used by the U.S. Further, that all data, manufacturing, and wiring details be furnished to the British for this purpose.

(e) That the British and U.S. make independent security studies of BRUTUS, including the following items:

(1) Possible changes in stepping order.

(2) Notch patterns for stepping control.

(3) Type of rotor wiring (interval, random, or composite).

(4) Preparation of key lists.

(5) Indicator procedure.

(6) Restrictions on operational use of machine for security reasons.

(7) And similar technical matters.

Further, upon completion of these studies the U.S. and the U.K. exchange technical papers through established channels.

(f) That the British and U.S. prepare and exchange separate papers for purpose of reaching agreements on operating instructions, maintenance instructions, crypto-security precautions, and other procedural matters.

(g) That models (when available), drawings, specifications, and operating instructions (where necessary) of the following equipments be made available to the British:

BCM (CSP 4800)

"PCM" (CSP 4700) and "PCM" type rotor

Tape Reader (AFSAM 12 or CSP 5100)

CSP 5000 Off-line automatic equipment

ENG-308 Translator for BCM (CSP 4800)

Rotor refinements for Mark I (3"), Mark II (3½"), and Mark III (2½") rotors

AN/GGA-1 (Instructions only)

Parts and drawings for the new TYPEX adapter

Temporary Improvement to the Existing CCM

(a) That ~~henceforth~~ there should be issued 20 rotors to the set for each existing CCM in lieu of present number of 10. This is to become effective as soon as practicable. Key lists should be so prepared that no rotor will ever be effective on two successive days, within the same key lists for each cryptochannel, so as to permit setting up two baskets for two successive days from a single set of 20 rotors thus obviating the need for duplicate sets of rotors. ~~(This will result in a substantial increase in the number of rotors to be fabricated under present plans.)~~

(b) That removable tires will be introduced as soon as practicable.

(c) That matters such as the rate of supersession and specific times of supersession be left to established agencies charged with such matters.

(d) That the U.S. make available to the ~~British~~ the tools and dies for Mark I rotors (for old TYPEX Adapter).

(e) That the U.S. make available to the British the tools and drawings of the old TYPEX adapter, together with drawings of the new design of TYPEX adapter rotors with tires.

Provision of combined working between British and U.S. crypto machines employing the BRUTUS technique and providing teleprinter facilities.

(a) That the Third Report of the Sub-Committee appointed to investigate this aspect be made available to the UK/US JCEC with the request that, as a matter of urgency, discussion be opened on what Teleprinter facilities should be provided in new Off-line Combined Cypher Machines which permit automatic encryption and decryption in page form.

(b) That the British, as a matter of urgency, give consideration to the U.S. proposal that bigramming and functional signals for British machines employing the BRUTUS crypto technique should be achieved by the use of the following primary characters:

Primary Character	Function	To Be Linked to
K	Bigram	D
J	Figure Shift	Y
V	Letter Shift	(Nothing)
Z	Space	X
C/R	Carriage Return	C
L/F	Line Feed	G

(c) That the U.S. consider the possibility of providing full Teleprinter facilities in future machines employing the BRUTUS crypto technique, by utilizing the Bigram function included in the design of the British "PENDRAGON".

(d) That since provision has been made in the British PENDRAGON for "Line Feed" and "Carriage Return" signals to be generated where required on decypherment by suitable counting mechanisms, the British should give consideration to abandoning Bigramming and accepting the loss of two lower case characters (J and Z) and three upper case characters (upper case J, upper case Z, and upper case V) as is at present contemplated in U.S. design.

(e) That interchange of views in particular on recommendations (b), (c), and (d) above be continued.

REPORT TO THE ~~BRITISH~~ U.K. AND US CHIEFS OF STAFF

~~BY THE BRITISH/US COMMUNICATIONS SECURITY CONFERENCE~~ ON THE REPLACEMENT OF THE CCM

SEPTEMBER 1950

Replacement for the present Combined Cypher Machine

1. As agreed by the British and US Chiefs of Staff* a British/US Conference to consider the replacement of the existing Combined Cypher Machine opened in Washington on the 21st September 1950, as a result of which the joint B representative recommended to

2. Many related cryptographic devices and features were demonstrated and discussed. Summaries of the proceedings at these meetings have been prepared and these are held both by the Director, Armed Forces Security Agency, Washington, and the Secretary, Cypher Policy Board, London.

~~3.~~ In our estimation this Conference has been of outstanding value in the field of Combined Communications Security. ~~and we would make the following general recommendations:~~

3. We recommended that

(a) ~~That~~ immediately and on a continuing basis there be complete interchange of technical details of the devices discussed in this conference. This should include technical visits.

(b) ~~That~~ there be annual conferences on this subject for the next four years, to be held alternately in London and in Washington, the first of these to take place in London in approximately nine months time.

* US Reference: JCS 2074/2 - 27 December 1949.
British Reference: COS (W) 831 - 25 August 1950.

(c) That the subject of Combined requirements for general point to point on-line encryption be introduced at the next Conference.

4. The general recommendations in paragraph 3 above together with the detailed technical recommendations conclusions of the conference which are attached as Appendix A to this report are submitted ~~with the recommendation that they be endorsed~~ for approval by the British and U.S. Chiefs of Staff.

APPENDIX A

TECHNICAL RECOMMENDATIONS

Replacement of the existing CCM

(a) That ~~the British accept~~ the cryptographic principles of the 7-rotor BCM (cryptosystem Brutus) be adopted as a replacement for the CCM in combined communications.

(b) That except by mutual agreement, disclosure of the 7-rotor BCM principle be limited to the U.S. and to the British Commonwealth, and that the British agree to notify the U.S. authorities when any issue of a combined 7-rotor BCM system is made to a nation of the British Commonwealth.

(c) That the target date for full implementation of the Brutus 7-rotor BCM be set as 1 January 1955, or sooner if circumstances permit, and that limited introduction, where a small number of machines would be involved, should be implemented at the earliest practicable date.

(d) That, insofar as practicable, rotors of ~~both~~ U.S. and British versions of the Brutus cryptosystems ~~7-rotor BCM~~ be physically and cryptographically interchangeable and that to this end the British should ~~change~~ adopt one of those of the pins to be used by the U.S. ~~to the size now used in CSP 1700~~. Further, that all data, manufacturing, and wiring details be furnished to the British for this purpose.

(e) That the British and U.S. make independent security studies of the Brutus 7-rotor BCM, including the following items:

(1) Possible changes in stepping order.

(2) Notch patterns for stepping control.

(3) Type of rotor wiring (interval, random, or composite).

(4) Preparation of key lists.

(5) Indicator procedure.

(6) Restrictions on operational use of machine for security reasons.

(7) And similar technical matters.

Further, upon completion of these studies the U.S. and the U.K. exchange technical papers through established channels.

(f) That the British and U.S. prepare and exchange separate papers for purpose of reaching agreements on operating instructions, maintenance instructions, crypto-security precautions, and other procedural matters.

(g) That models (when available), drawings, specifications, and operating instructions (where necessary) of the following equipments be made available to the British:

BCM (CSP 4800)

"PCM" (CSP 4700) and "PCM" type rotor

Tape Reader (AFSAM 12 or CSP 5100)

CSP 5000 Off-line automatic equipment

ENG-308 Translator for BCM (CSP 4800)

Rotor refinements for Mark I (3"), Mark II (3½"), and Mark III (2½") rotors

AN/GGA-1 (Instructions only)

Parts and drawings for the new TYPEX adaptor

Temporary Improvement to the Existing CCM

(a) That ~~henceforth~~ as soon as practicable there should be issued 20 rotors to the set for each CCM in lieu of present number of 10. ~~This to become effective with the next issue of new rotors.~~ Key lists should be so prepared that no rotor will ever be effective on two successive days, within the same key lists for each cryptochannel, so as to permit setting up two baskets for two successive days from a single set of 20 rotors thus obviating the need for duplicate sets of rotors. ~~(This will result in no substantial increase in the number of rotors to be fabricated under present plans.)~~

(b) That removable tires will be introduced as soon as practicable, ~~after suitable rotors become available~~.

(c) That matters such as the rate of supersession and specific times of supersession be left to established agencies charged with such matters.

(d) That the U.S. make available to the British the tools and dies for Mark I rotors (for old TYPEX Adapter).

(e) That the U.S. make available to the British the tools and drawings of the old TYPEX adapter, together with drawings of the new design of TYPEX adapter rotors with tires.

Provision of combined working between British and U.S. crypto machines employing the 7-rotor B.C.M. technique and providing teleprinter facilities.

(a) That the Third Report of the Sub-Committee appointed to investigate this aspect be made available to the UK/US JCEC with the request that, as a matter of urgency discussion be opened on what Teleprinter facilities should be provided in new Off-line Combined Cypher Machines which permit automatic encrption and decryption in page form.

(b) That the British as a matter of urgency give consideration to the U.S. proposal that bigramming and functional signals for British machines employing the 7-rotor B.C.M. crypto technique should be achieved by the use of the following primary characters:

Primary Character	Function	To Be Linked to
K	Bigram	D
J	Figure Shift	Y
V	Letter Shift	
Z	Space	X
C/R	Carriage Return	C
L/F	Line Feed	G

(c) That the U.S. as a matter of urgency consider the possibility of providing full Teleprinter facilities in future machines employing the 7-rotor B.C.M. crypto technique, by utilizing the Bigram function

included in the design of the British "PENDRAGON".

(d) That since provision has been made in the British PENDRAGON for "Line Feed" and "Carriage Return" signals to be generated where required on decypherment by suitable counting mechanisms, the British should give consideration to abandoning Bigramming and accepting the loss of two lower case characters (J and Z) and three upper case characters (upper case J, upper case Z, and upper case V) as is at present contemplated in U.S. design.

(e) That interchange of views in particular on recommendations (c), (d), and (e) above be continued through existing channels.